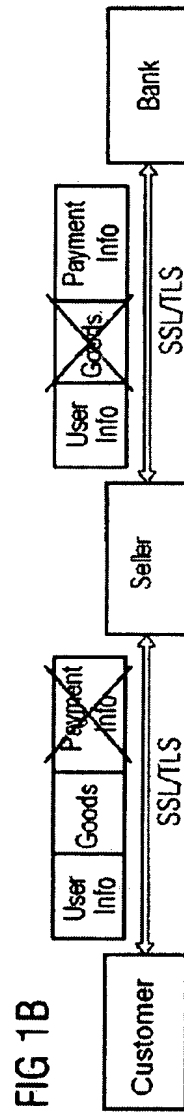
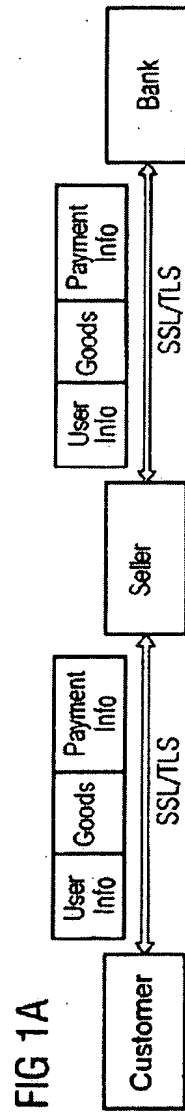


1/9



2/9

FIG 2A

Attribute	Encrypted Attribute Extension
VISA	$E(K_{\text{VISAPublicKey}}, \text{CreditCardNumber})$
American Express(AMEX)	$E(K_{\text{AMEXPublicKey}}, \text{CreditCardNumber})$
MasterCard	$E(K_{\text{MasterCardPublicKey}}, \text{CreditCardNumber})$
Bank Account	$E(K_{\text{BankPublicKey}}, \text{AccountNumber})$
Address	$E(K_{\text{PostPublicKey}}, \text{Address})$
Social Insurance Number	$E(K_{\text{InsurancePublicKey}}, \text{InsuranceNumber})$

Table 1.1: New certificate extensions.

FIG 2B

OID	Value
1.3.6.1.4.15601	Root node of new extensions
1.3.6.1.4.15601.1	Encrypted value: VISA credit card number
1.3.6.1.4.15601.2	Encrypted value: American Express credit card number
1.3.6.1.4.15601.3	Encrypted value: MasterCard credit card number
1.3.6.1.4.15601.4	Encrypted value: Bank account number
1.3.6.1.4.15601.5	Encrypted value: Address
1.3.6.1.4.15601.6	Encrypted value: Social insurance number

Table 1.2: New private OIDs.

FIG 3A

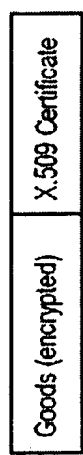


FIG 3B

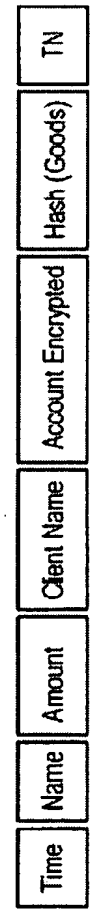


FIG 3C

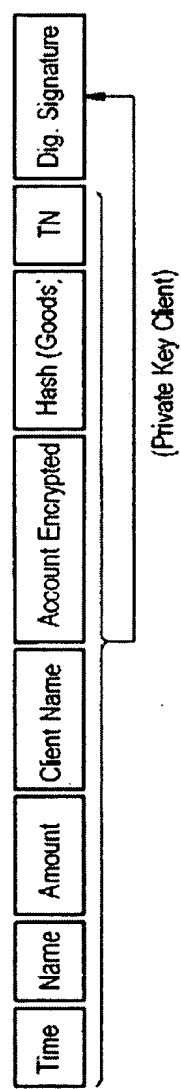


FIG 3D

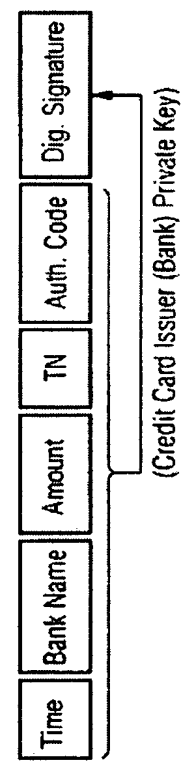


FIG 3E

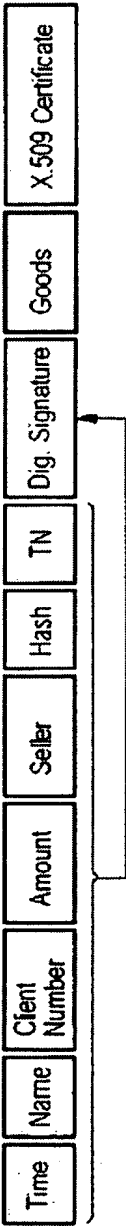


FIG 3F

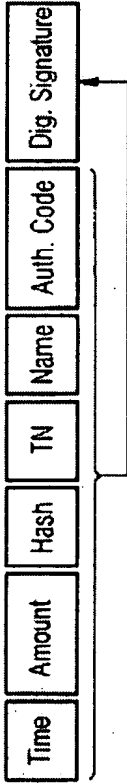


FIG 3G

User request format:

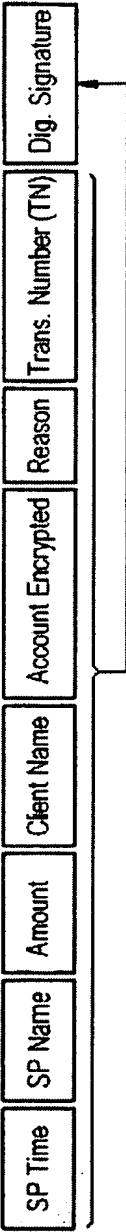
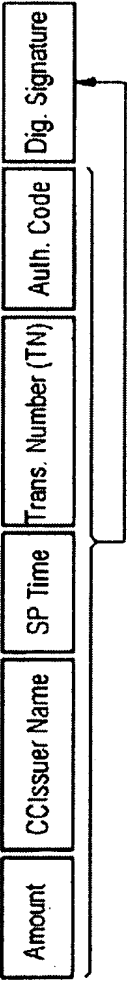


FIG 3H

Credit Card Issuer response format:



5/9

FIG 4

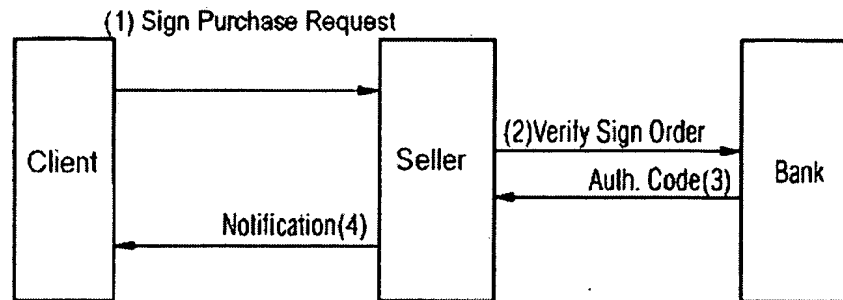
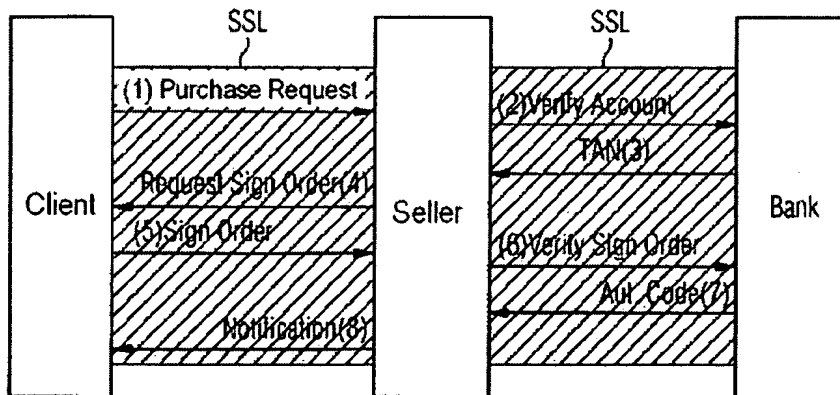
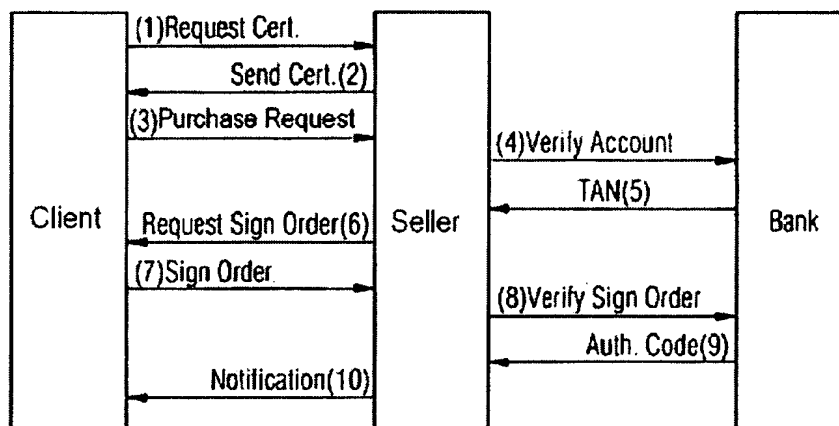


FIG 5

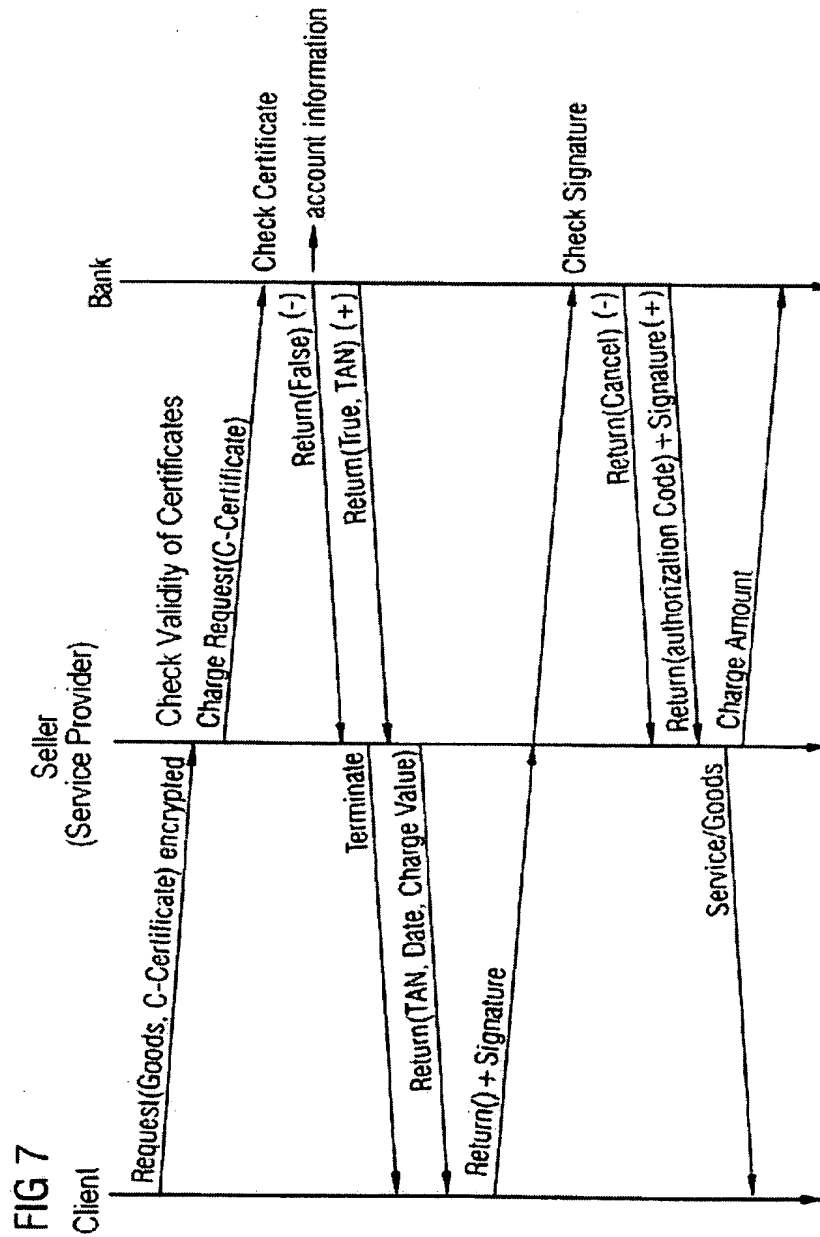


6/9

FIG 6



7/9



8/9

FIG 8

